



# **Information Law: Cases and Materials Volume Two**

**Professor Lisa M. Austin  
Faculty of Law, University of Toronto  
Winter 2005**

**These materials are reproduced solely for the use of students in the Faculty of Law,  
University of Toronto  
2004-2005**

BORA LASKIN LAW LIBRARY

JAN - 3 2005


FACULTY OF LAW  
UNIVERSITY OF TORONTO

# **Information Law: Cases and Materials**

## **Volume Two**

**Professor Lisa M. Austin**  
**Faculty of Law, University of Toronto**  
**Winter 2005**

**These materials are reproduced solely for the use of students in the Faculty of Law,  
University of Toronto  
2004-2005**



Digitized by the Internet Archive  
in 2018 with funding from  
University of Toronto

<https://archive.org/details/informationlawca02aust>

# Information Law: Cases and Materials Volume Two

## Table of Contents

### *A. Access to Information Act*

#### **Threshold Question: Records under Control of Government Institutions**

<i>Canada Post Corp. v. Canada (Minister of Public Works) (C.A.)</i> , [1995] 2 F.C. 110 .....	1
<i>Canada (Attorney General) v. Canada (Information Commissioner)</i> , [2004] F.C.J. No. 524.....	11
Notes: .....	26
<i>Canada (Privacy Commissioner) v. Canada (Labour Relations Board)</i> [2000] F.C.J. No. 617. ....	26

#### **Overview of Exemptions and Exclusions..... 28**

#### **Exclusions (ss. 68-69)**

<i>Babcock v. Canada (Attorney General)</i> 2002 SCC 57 .....	29
<i>Canada (Information Commissioner) v. Canada (Minister of the Environment)</i> 2003 FCA 68.....	40
Notes .....	45
Public Records .....	45

#### **Exemptions: Secrecy in Governance**

<i>Canada (Information Commissioner) v. Canada (Prime Minister) (T.D.)</i> [1993] 1 F.C. 427.....	49
The Amber Light Process .....	63

#### **Exemptions: Confidential Information**

<i>Canadian Tobacco Manufacturers' Council v. Canada (Minister of National Revenue - M.N.R.)</i> 2003 FC 1037 .....	68
Notes .....	81
Drug Information .....	81

#### **Exemptions: Personal Information**

<i>Dagg v. Canada (Minister of Finance)</i> [1997] 2 S.C.R. 403.....	82
<i>Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)</i> 2003 SCC 8.....	106
<i>Reporters Committee for Freedom of the Press v. United States Department of Justice</i> , 489 U.S.749 (1989).....	111
<i>Canada (Information Commissioner) v. Canada (Minister of Public Works and Government Services) (T.D.)</i> , [1997] 1 F.C. 164 .....	122
Notes .....	127
Census Information.....	127

## ***B. The Privacy Act***

### **Access to Personal Information**

<i>Ruby v. Canada (Solicitor General) 2002 SCC 75</i> .....	129
---	-----

### **Collection, Use and Disclosure of Personal Information**

<i>Privacy Act (Can.) (Re) (C.A.) [2000] 3 F.C. 82</i> .....	154
CUB 44824 .....	158
<i>Smith v. Canada (Attorney General)</i> , 2001 SCC 88 .....	178
Opinion by retired Supreme Court Justice Hon. Gerard V. LaForest, C.C., Q.C., re: CCRA Passenger Name Record (footnotes removed) .....	179
Notes: .....	190
(a) Subsequent Developments in the CCRA database .....	190
(b) Recent Developments in Government Information-Sharing Practices .....	193

## ***C. Personal Information and Protection of Electronic Documents Act***

### **Personal Information**

PIPED Act Case Summary #4 .....	198
PIPED Act Case Summary #25 .....	200
PIPED Act Case Summary #99 .....	202
Notes .....	210
(a) Anonymity .....	210
(b) Information About Third Parties .....	210
(c) Genetic Information and Third Parties .....	211

### **Knowledge, Consent and Reasonable Purposes**

PIPED Act Case Summary # 42 .....	212
Current Air Canada Aeroplan Privacy Policy .....	217
<i>Englander v. Telus Communications Inc.</i> , 2004 FCA 387. ....	229
PIPED Act Case Summary #65 (Employer accused of forcing consent to security screening) .....	248
<i>L'Ecuyer v. Aéroports de Montréal</i> , 2003 FCT 573 .....	250
<i>Eastmond v. Canadian Pacific Railway</i> , 2004 FC 852 .....	253
PIPED Act Case Summary #48 (Applicant for service objects to providing credit card or bank account information) .....	273
Notes: .....	275
1) Consent and Employee Privacy: Provincial Legislation .....	275
2) Video Surveillance Activities in a Public Place .....	275

### **Exceptions from Consent**

PIPEDA Case Summary #264 (Video cameras and swipe cards in the workplace) .....	276
PIPEDA Case Summary #265 (Video cameras in the workplace) .....	279
PIPEDA Case Summary #269 (Employer hires private investigator to conduct video surveillance on employee) .....	281

<i>Public Safety Act</i> Amendments to PIPEDA.....	285
--	-----

## **Accuracy and Access**

PIPED Act Case Summary #53(Bank accused of providing police with surveillance photos of the wrong person) .....	286
PIPED Act Case Summary #73 (Telecommunications company asked to adopt consistent retention practices).....	289

## Notes:

### ***Canada (Privacy Commissioner) v. Canada (Labour Relations Board)* [2000] F.C.J. No. 617.**

The Canada Labour Relations Board refused to disclose to the Privacy Commissioner of Canada notes taken by members of the Board during a hearing of a complaint of a breach of a duty of fair representation under the Canada Labour Code. The Federal Court determined that these notes were not under the control of the Labour Board, as required by the Privacy Act. In determining this, the Court argued, at paras. 5-8:

... These notes are being taken during the course of quasi-judicial proceedings, not by employees of the Board, but by Governor in Council's appointees endowed with adjudicative functions which they must perform, not as agent of the Board, but independently of other members of the Board including the chairperson of the Board or a government institution. Board members are under no obligation to take notes although they may. Their notes are not part of the official records of the Board and are not contained in any other record keeping system over which the Board has control.

The trial judge made the following statement with which we agree:

... It is clear that there is no requirement either in the Canada Labour Code, or in the CLRB policy or procedure touching upon the notes. The notes are viewed by their authors as their own. The CLRB members are free to take notes as and when they see fit, and indeed may simply choose not to do so. The notes are intended for the eyes of the author only. No other person is allowed to see read or use the notes, and there is a clear expectation on the part of the author that no other person will see the notes. The members maintain responsibility for the care and safe keeping of the notes and can destroy them at any time. Finally, the notes are not part of the official records of the CLRB and are not contained in any other record keeping system over which the CLRB has administrative control.

In my view, it is apparent from the foregoing that however broadly one construes the word control, the notes in issue were not "under the control" of the CLRB within any of the meanings that can be attributed to that term. Not only are the notes outside the control or custody of the CLRB but they are also considered by the CLRB to fall outside the ambit of its functions.

Paragraphs 15(a) and (q) of the Canada Labour Code empower the Board to make regulations with respect to:

- a) the establishment of rules of procedure for its hearing;

...



- q) such other matters and things as may be incidental or conducive to the proper performance of the duties of the Board under this part.

We agree with the trial judge's conclusion that, by means of this power, the Board could not exercise such control over these notes as to bring them "under the control of a government institution" within the meaning of paragraph 12(1)(b) of the Privacy Act.

## Overview of Exemptions and Exclusions

<b>Mandatory exemptions</b>	<ul style="list-style-type: none"> <li>• Information received in confidence from other governments (13)</li> <li>• Information obtained or prepared by RCMP re: provincial or municipal policing services (16(3))</li> <li>• <b>Personal information (19)*</b></li> <li>• Trade secrets of Third Party (20(1)(a))</li> <li>• Financial, commercial, scientific or technical information received in confidence from Third Party (20(1)(b))*</li> <li>• Information protected under other, listed statutes (24)</li> </ul>	<ul style="list-style-type: none"> <li>• Loss or gain to Third Party or prejudice to competitive position (20(1)(c))*</li> <li>• Interference with contractual or other negotiations of Third Party (20(1)(d))</li> </ul>
<b>Discretionary exemptions</b>	<ul style="list-style-type: none"> <li>• Information obtained or prepared by listed investigative bodies (16(1)(a))</li> <li>• Information on techniques or plans for investigations (16(1)(b))</li> <li>• Trade secrets or valuable financial, commercial, scientific or technical information of Canada (18(a))</li> <li>• Advice or recommendations to government (21(1)(a))</li> <li>• Account of consultations or deliberations (21(1)(b))</li> <li>• Government negotiation plans (21(1)(c))</li> <li>• Government personnel or organizational plans (21(1)(d))</li> <li>• Solicitor-client privileged information (23)</li> <li>• Information to be published in 90 days (26)</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Injury to conduct of federal-provincial affairs (14)</b></li> <li>• Injury to conduct of international affairs, or to defence of Canada or allied states (15)</li> <li>• Injury to law enforcement or conduct of lawful investigations (16(1)(c))</li> <li>• Harm in facilitating commission of criminal offence (16(2))</li> <li>• Threat to individual's safety (17)</li> <li>• Prejudice to competitive position of government (18(b))</li> <li>• Harm in depriving government researcher of priority of publication (18(c))</li> <li>• Injury to financial or economic interests of Canada (18(d))</li> <li>• Prejudice to use of audits or tests (22)</li> </ul>

\* Denotes mandatory exemptions which include a public interest override, i.e., the information may be disclosed where the public interest in disclosure outweighs the interest protected by the exemption.

(Source: *Access to Information: Making it Work for Canadians*, Report of the Access to Information Review Task Force, June 2002.)

### Exclusions under the Access to Information Act (ss. 68-69)

- Published material or material available to the public for purchase (s.68(a))
- Library, museum, or archival materials (s.68(b) and (c))
- Cabinet confidences (s.69)
- Information subject to a *Canada Evidence Act* certificate (s.69.1)





## Notes

### Drug Information

(From “Confidentiality Versus Public Interest,” Office of the Information Commissioner of Canada Annual Report: 2003-2004)

### Background

The Canadian Institute of Health Research awarded funds to the University of British Columbia to conduct research on the health risks to healthcare workers of certain disinfectant products. As part of the research, a UBC researcher made an access request to Health Canada for toxicological data on a disinfectant known as CIDEX OPA solution, manufactured by Johnson & Johnson.

Health Canada disclosed some information, but withheld most details in order to protect the manufacturer from commercial and competitive injury.

The researcher complained to the Information Commissioner arguing that the public interest in determining the risks of the product to public health and safety should override the manufacturer’s commercial and competitive concerns.

### Legal Issue

Did Health Canada properly exercise the discretion given to it by subsection 20(6) of the *Access to Information Act*? That provision authorizes government to disclose commercially sensitive information "if that disclosure would be in the public interest as it relates to public health, public safety or the protection of the environment and, if the public interest in disclosure clearly outweighs in importance any financial loss or gain to, prejudice to the competitive position of or interference with contractual or other negotiations of a third party."

The researcher seeking disclosure argued that disinfectants, like CIDEX OPA solution, might have an adverse effect on the health of healthcare workers. She argued that the goal of the research--that of comparing the relative health impacts of various products--was supported by the Workers’ Compensation Board of B.C., the Occupational Health and Safety Agency for Healthcare in B.C., healthcare management associations, and labour union members.

For its part, Health Canada took the position that the requester had not shown that the product in question poses any threat to public health or safety. Health Canada and the product’s manufacturer took the view that the approved labeling and package insert for the product ensure that the product is handled and used safely. In the absence of some evidence to the contrary, they argued that disclosure would not promote any public interest and, hence, would not outweigh the likely commercial prejudice to the manufacturer from disclosure of the toxicological data.

The commissioner agreed with Health Canada and Johnson & Johnson that this was not a case where the public interest in health and safety outweighed the commercial and competitive interests of Johnson & Johnson. The commissioner found that Health Canada had carefully weighed the factors for and against disclosure and that there was good reason to insist on secrecy in this case. The complaint was recorded as not substantiated.

### Lessons Learned

Government institutions are under a mandatory obligation to refuse to disclose information if disclosure could harm private firms. They are also under an obligation to consider the subsection 20(6) public interest override before refusing access. This discretion to disclose in the public interest must be exercised in good faith and there must be evidence that relevant factors for and against disclosure were weighed. If the discretion to disclose in subsection 20(6) is exercised in good faith, it is not for the commissioner or a reviewing court to seek to substitute its judgment for that of the head of the government institution which received the access request.

### Exemptions: Personal Information

#### *Dagg v. Canada (Minister of Finance) [1997] 2 S.C.R. 403*

The judgment of Lamer C.J. and Sopinka, Cory, McLachlin and Iacobucci JJ. was delivered by

¶ 1 CORY J.:— I have read the careful and extensive reasons of Justice La Forest. I agree with his approach to the interpretation of the Access to Information Act, R.S.C. 1985, c. A-1, and the Privacy Act, R.S.C., 1985, c. P-21, particularly that they must be interpreted and read together. I also agree that the names on the sign-in logs are "personal information" for the purposes of s. 3 of the Privacy Act. However, I arrive at a different conclusion with respect to the application of s. 3 "personal information" (j) (hereinafter s. 3(j)) of that Act.

¶ 2 Subsection 3(j) of the Privacy Act provides that:

... for the purposes of sections 7, 8 and 26 and section 19 of the Access to Information Act, ["personal information"] does not include

(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

...

(iii) the classification, salary range and responsibilities of the position held by the individual,

(iv) the name of the individual on a document prepared by the individual in the course of employment. . . .







## Notes

### Census Information

#### ***The Information Commissioner of Canada v. The Minister of Industry Canada, (T-0053-04)***

Federal Court

Nature of Action

This is an Application for Judicial Review under section 42 of the Access to Information Act of a refusal, by Statistics Canada, through the delegated authority of the Minister of Industry Canada, to release some returns from the 1911 Census.

#### Factual Background

On May 29, 2002, a citizen requested access to the 1911 Census records for two specific regions in Ontario. Arguing that the records are exempt from disclosure pursuant to sections 19 and 24 of the Act, which makes reference to section 17 of the Statistics Act, Statistics Canada refused disclosure. After investigating the resulting complaint, the Information Commissioner recommended disclosure of the requested records. Statistics Canada refused to follow the commissioner's recommendation.

On January 12, 2003, the Information Commissioner of Canada filed an Application for Judicial Review of the decision to refuse access. During the month of February, the commissioner filed his affidavit evidence in support of the application.

#### Issues Before the Court

Did the respondent err in relying on section 24 of the Act and section 17 of the Statistics Act to refuse to disclose the Perth County, Ontario Census nominal returns for 1911? Are the privacy interests in historical census records determined by paragraphs 19(2)(b) and (c) of the Access to Information Act, by paragraph 8(2)(j) and subsection 8(3) of the Privacy Act and section 6 of the Privacy Regulations?

(From Office of the Information Commissioner of Canada Annual Report 2003-2004)

#### ***The Information Commissioner of Canada v. The Minister of Industry Canada, (T-0421-04)***

Federal Court

Nature of Action

This is an Application for Judicial Review by the Information Commissioner under section 42 of the *Access to Information Act* of a refusal, by Statistics Canada, through the delegated authority of the Minister of Industry Canada, to release the 1911, 1921,

1931 and 1941 Census records. Statistics Canada relied on section 24 of the Act as well as section 17 of the *Statistics Act* to justify the refusal to disclose.

### Factual Background

On November 2, 2001, a native claim researcher requested access to the 1911, 1921, 1931 and 1941 Census records for specific districts in Quebec and Ontario. Arguing that the records are exempt from disclosure pursuant to section 24 of the Act, which makes reference to section 17 of the *Statistics Act*, Statistics Canada refused disclosure. After investigating the resulting complaint, the Information Commissioner recommended disclosure of the requested records. Statistics Canada refused to follow the commissioner's recommendation.

On February 26, 2004, the Information Commissioner filed an Application for Judicial Review of the decision to refuse access. During the month of February, the commissioner filed its affidavit evidence in support of the application.

### Issues Before the Court

Did the respondent err in relying on section 24 of the Act and section 17 of the *Statistics Act* to refuse disclosure of the Census returns?

To the extent that the information is subject to section 17 of the *Statistics Act*, did the respondent properly exercise his discretion under subsection 17(2) of the *Statistics Act*? Are the 1911 Census records deemed to be publicly available pursuant to paragraph 19(2)(b) of the Act?

Is access to the Census returns of 1911, 1921, 1931 and 1941 authorized pursuant to paragraph 19(2)(c) of the Act by reference to paragraph 8(2)(k) and subsection 8(3) of the *Privacy Act* and section 6 of the Privacy Regulations?

(From Office of the Information Commissioner of Canada Annual Report 2003-2004)



## Notes:

### (a) Subsequent Developments in the CCRA database

On April 9, 2003, the Privacy Commissioner of Canada, George Radwanski, issued the following statement, and made public the following letter from the Honourable Elinor Caplan, Minister of National Revenue, regarding changes to what he has previously described as the Canada Customs and Revenue Agency's "Big Brother" database:

#### Commissioner's Statement

Revenue Minister Elinor Caplan's letter to me today announcing major policy changes regarding the Canada Customs and Revenue Agency's new six-year passenger information database is an important moment in the history of privacy protection in Canada.

Since last summer, I have been expressing grave privacy concerns about the creation of this database containing extensive information, obtained from airlines, on the foreign travel activities of all law-abiding Canadians – more than 30 data elements including where and with whom we travel, method of payment for tickets, contact addresses and telephone numbers, even dietary and health-related requirements communicated to the airlines.

I was particularly concerned that, under the information-sharing provisions of the Customs Act, all this information would have been available for a virtually unlimited range of governmental and law enforcement purposes. Such purposes, by the Government's own account, could for instance have included routine income tax investigations and flagging individuals as possible pedophiles on the basis of repeated travel to countries that have a flourishing child sex trade.

Now there will be no such dossiers of personal information obtained from third parties about the lawful activities of all Canadians, for unrestricted potential future use against any individual. A precedent-setting and extraordinarily grave intrusion on privacy rights has been averted.

The changes announced today by Minister Caplan very substantially address the concerns expressed by myself and many others.

They effectively eliminate the use of this information for fishing expeditions such as identifying everyone who has travelled to a particular country a certain number of times, or routinely accessing travel profiles of individuals for tax review purposes. They eliminate meal and health information outright. And they very significantly limit the use and sharing of personal information about travel activities.

This is a great victory for the privacy rights of all Canadians.

It would, of course, be preferable from a privacy perspective not to have this database at all, or to have it absolutely restricted to anti-terrorism purposes. But the changes announced by Minister Caplan strike a fair and reasonable balance between the responsibilities of CCRA, particularly with regard to maintaining border security against terrorism, and the privacy rights of Canadians. The information is now to be kept only for purposes that are consistent with the CCRA's mandate, and it is to be used and shared only subject to appropriate limitations and safeguards.

Minister Caplan has demonstrated that she is sensitive to the importance of privacy rights in Canadian society, and for this I am deeply appreciative.

Today's announcement also demonstrates that the Canadian approach to privacy protection, based on an ombudsman model that combines behind-the-scenes persuasion and dialogue with recourse to public debate and other initiatives when necessary, is a very good and effective one.

In summary, I have been informed by Minister Caplan and the CCRA that the database will henceforth function as follows:

Advance Passenger Information (API) – which consists only of passport information such as name and date of birth and does not include any specific travel information – will continue to be stored for six years and can be widely shared under Section 107 of the Customs Act.

The much more detailed Passenger Name Record (PNR) – which contains all the information held by an airline – will immediately be purged by the CCRA of all meal and health information.

PNR data will still be held for six years, but use and access will vary by length of retention, which is divided into three time periods.

For the first 72 hours, it will be used by customs and immigration officers to assess risk, as at present.

From 72 hours to two years, the information will be depersonalized and used, without names attached, only by intelligence officers and analysts. The information can be re-identified with the traveller's name only when necessary for customs purposes.

During this two-year period, information will only be shared with other agencies or departments for non-customs purposes if a warrant has been obtained. This includes the tax side of the CCRA.

Where the information relates to a customs offence, the CCRA will disclose it to law enforcement authorities on its own initiative. And it will share information with other countries, to assist with a customs investigation, in accordance with written agreements.

From two years to six years, the information can only be used to fulfill the CCRA's mandate regarding the security of Canada, rather than all customs purposes. It will be used on a depersonalized basis unless the Commissioner of the CCRA personally approves re-personalizing it based on reason to suspect that the name or other identifying elements are necessary to deal with a high-risk person.

During this final period, information can only be shared with agencies that have a national security or defence mandate, where there are reasonable grounds to believe that the information relates to a real or apprehended threat.

The combined effect of all these changes is to transform the CCRA database from an open-ended, unrestricted intrusion on privacy into a much more nuanced, restrained and appropriate instrument. I have communicated my appreciation to Minister Caplan, CCRA Commissioner Rob Wright and other senior Government officials for having achieved this favourable outcome that will benefit all Canadians.



## Notes

### (a) Anonymity

**Sweeney, Latanya. "Weaving Technology and Policy Together to Maintain Confidentiality". *The Journal of Medicine and Ethics* Vol. 25: 2 & 3 (Summer and Fall) 1997.**

Sweeney discusses the difference between de-identified data and anonymous data. The former refers to data that has had identifiers, such as name, address or SSN removed, while the latter is data that cannot be manipulated or interpreted such that it is re-linked with identifying features. The distinction in these definitions points to some of the problematic dimensions of anonymizing data in order to protect confidentiality. The author points to three major problems in providing anonymous data:

Anonymity is in the eye of the beholder, that is there is no way to know what knowledge the receiver of data will bring to its interpretation. Even with the absence of names, certain identifiers can be used to re-link the data with the identity. For example, if the data includes an ethnic descriptor and a postal code and the researcher was familiar with the ethnic make-up of the neighbourhood, identification becomes easier.

In any collection of data, unique characteristics can be used in conjunction with other identifiers to destroy anonymity. Sweeney uses the example of a clinic where there is only one patient under 45. Assuming that the user of the data knew its source, anonymity of this individual is non-existent because of his/her uniqueness within the data set.

Measuring the degree of anonymity depends on the size of the data set. The larger the "bin size" of the set that can be identified by combining identifiers, the greater the degree of anonymity. The determination of optimal bin size is complex and depends on the difference between the information contained in the data set and other available information that can be applied to re-link the data with an identity, which is often not known before hand.

In conclusion, Sweeney notes that recognition of the capacity to identify "anonymous" data through re-linking is a step towards producing policies that protect individuals' privacy and confidentiality, while still ensuring that data is available for research purposes. She advocates the implementation a central bank of health data that could be monitored by an agency to ensure optimal anonymity by limiting identifier re-linking.

### (b) Information About Third Parties

A complaint was made to the Privacy Commissioner regarding an employer's collection of spousal information without spousal consent. (PIPED Act Case Summary #232). An employee of a nuclear facility complained that his employer was requiring employees to provide personal information of spouses or common-law partners for the purpose of a security clearance check without the spouse's or partner's consent. The Privacy Commissioner determined that the collection of this information was reasonable. With respect to spousal consent, the case summary indicates:

the Commissioner determined that it would not be appropriate for the company to obtain separate consent. In his view, the onus is on the employee to discuss the matter with the spouse or partner and seek consent. Should the spouse or partner not agree, the employee would need to review their options, such as seeking alternative employment. To suggest that the company should obtain separate consent could lead to a situation in which the employee is investigated while the partner is not. Such a scenario would clearly result in the failure to achieve the purposes of conducting the check — purposes already deemed to be entirely appropriate.

### **(c) Genetic Information and Third Parties**

The nature of genetic information, including tests for genetic conditions, hereditary characteristics and traits and DNA profiles, is such that its influence can extend to parties other than the individual whose information is directly involved or known. For example, the information contained in an individual's genetic code shares characteristics and qualities with that of his or her family members and on an even broader perspective with his or her ethnic community or group. This dimension of genetic information injects a critical health policy consideration into developing regulations for disclosure of information. Issues such as a family member's likelihood of developing a hereditary health condition and thus seeking preventative treatment become problematic when the diagnostic information comes from a separate individual's personal health information. Another example of the involvement of third party interests in genetic information is paternity tests where disclosed information can cross confidentiality boundaries when personal information is brought under public scrutiny without the mother or father's permission.

Population-based genetic studies of ethnic groups and communities involve another collective interest in genetic information is found. Proof of shared cultural heritage can be found in genetic codes, such as the proof of the South African Lembe community's Jewish heritage which was based on a common chromosome. Of course, inclusion in a group can be based on shared cultural identifiers as much as shared genes and a scientific analysis of group's genetics can prove culturally problematic. Use of group DNA patterns also raises important issues with regards to informed consent and the use of the information contained in genes. How can a group of individuals consent to how its genetic information is managed when there are so many separate and possibly conflicting individual interests at stake? Some of the unique qualities of genetic information and the potential for conflict between individual privacy and confidentiality and third party and collective interests makes the need for clear policy considerations in the disclosure and use of such data obvious.

(from Lemmens, Trudo and Lisa Austin. "The Challenges of Regulating the Use of Genetic Information". *ISUMA* 2(3) (2001): 26-37.)





## Notes:

### 1) Consent and Employee Privacy: Provincial Legislation

Both British Columbia and Alberta have introduced legislation to protect the privacy of personal information. Both pieces of legislation define and treat employee personal information differently from individual personal information outside the employment context: *Personal Information Protection Act*, S.B.C. 2003, c.63 (British Columbia) and *Personal Information Protection Act*, S.A. 2003, c.P-6.5 (Alberta). Both Acts define personal employee information similarly as being information collected, used or disclosed by an organization that reasonably relates to the establishment, management and termination of the employment relationship. Both permit the collection, use or disclosure of personal employee information without employee consent where the action taken is for a reasonable purpose relating to the employment relationship and notice is given. The British Columbia and Alberta Acts were deemed “substantially similar” to PIPEDA: *Organizations in the Province of British Columbia Exemptions Order*, C.Gaz.2004.I.1178 (unregistered) and *Organizations in the Province of Alberta Exemption Order*, C.Gaz.2004.I.1174 (unregistered).

However, in his evaluation of the “substantially similar elements of proposed provincial legislation” that is required under PIPEDA, the former Privacy Commissioner George Radwanski criticized the lack of protection for privacy that the proposed Acts provided to employees. Holding that consent with regards to one’s personal information is the cornerstone of privacy, he alleged that the reasonability requirement is a weak test for ensuring privacy of personal employee information, since “an employer could argue that almost any intrusion on employee privacy is ‘reasonable’ in the sense of establishing, managing or terminating the employment relationship”. He situated his criticism in a comparison with the protection granted under PIPEDA, which does not distinguish between information collected, used or disclosed in the commercial versus the employment contexts. The PC also noted that while an employee could complain of an unreasonable action taken with regards to their personal information, the violation of privacy would already have occurred leaving a limited remedy available.

### 2) Video Surveillance Activities in a Public Place

(Summary of PIPED Act Case #1)

The complaint centered on the live video monitoring of a major intersection in Yellowknife as a marketing demonstration by the security company in question. Since the monitoring involved the activities of people, it was held to be personal information for the purposes of the Act and since the recorded individuals did not consent, the company was in contravention of the Act. The Privacy Commissioner noted that “[t]here may be instances where it is appropriate for public places to be monitored for public safety reasons. But this must be limited to instances where there is a demonstrable need. It must be done only by lawful public authorities and it must be done only in ways that incorporate all privacy safeguards set out by law. There is no place in our society for unauthorized surveillance of public places by private sector organizations for commercial reasons.”

